structure on paths ranging from roots to leaves of the key tree structure, and wherein the device is associated with one of the leaf keys, and wherein said enciphering data further comprises upper-rank keys to be enciphered by lower-rank keys; and

wherein, the memory device stores a key distribution approval data file comprising header data, which comprises a link count key for designating a number of contents data that should be enciphered by the enciphering data acquirable from the enabling key block distribution authenticating key.

16. (New) The apparatus according to claim 15, wherein the key distribution approval data file comprises a contents key enciphering key (E (KEK, Kcon)) comprising a contents data enciphering contents key (Kcon) enciphered by the key enciphering key (KEK).

17. (New) The apparatus according to claim 15, wherein the memory device updates the link count key in correspondence with a variation in the number of contents data.

18. (New) The apparatus according to claim 15, wherein the memory device stores a key enciphering key, wherein the key enciphering key is acquired by decoding the enabling key block distribution authenticating key contained in a key distribution approval data file having a greater count number value for the link-count key than other key distribution approval data files stored in the memory device.

19. (New) The apparatus according to claim 15, wherein the memory device stores a key enciphering key, wherein the key enciphering key is acquired by decoding the enabling key block distribution authenticating key contained in a key distribution approval data file having a greater count number value for the

link-count key than other key distribution approval data files stored in the memory device, and wherein the device uses the key enciphering key if it is applicable to the contents data and the other key distribution approval data files otherwise.

20. (New) The apparatus according to claim 15, wherein the wherein the enabling key block distribution authenticating key enciphered by the enabling key block is subject to a version controlling process by way of executing a process for renewing individual versions on the device.

A1

21. (New) The apparatus according to claim 15, wherein the device enciphers a plurality of the leaf keys and then stores the enciphered leaf keys in a memory of the device.

22. (New) The apparatus according to claim 15, wherein the device further comprises a memory for storing a device key block, and wherein the device key block corresponds to an assemblage of enciphered keys comprising mutually different node keys, of the key tree structure, that are individually enciphered.

23. (New) A method for use in recording data to, or reproducing data from, a memory device, the method comprising the steps of:

enciphering an enabling key block distribution authenticating key by an enabling key block comprising enciphering data for enciphering renewal keys on paths of a hierarchical key tree structure comprising a variety of keys disposed in correspondence with roots, nodes, and leaves of the key tree structure on paths ranging from roots to leaves of the key tree structure, and wherein a device is associated with one of the leaf keys, and wherein said enciphering data further

comprises upper-rank keys to be enciphered by lower-rank keys; and

storing, in the memory device, a key distribution approval data file comprising header data, which comprises a link count key for designating a number of contents data that should be enciphered by the enciphering data acquirable from the enabling key block distribution authenticating key.

24. (New) The method of claim 23, wherein wherein the key distribution approval data file comprises a contents key enciphering key (E (KEK, Kcon)) comprising a contents data enciphering contents key (Kcon) enciphered by the key enciphering key (KEK).

A1

25. (New) The method of claim 23 further comprising the step of updating the link count key in correspondence with a variation in the number of contents data.

26. (New) The method of claim 23 further comprising the step of storing a key enciphering key, wherein the key enciphering key is acquired by decoding the enabling key block distribution authenticating key contained in a key distribution approval data file having a greater count number value for the link-count key than other key distribution approval data files stored in the memory device.

27. (New) The method of claim 23 further comprising the steps of:

storing a key enciphering key, wherein the key enciphering key is acquired by decoding the enabling key block distribution authenticating key contained in a key distribution approval data file having a greater count number value for the

link-count key than other key distribution approval data files stored in the memory device, and

using the key enciphering key if it is applicable to the contents data and using the other key distribution approval data files otherwise.

28. (New) A computer-readable medium for storing computer-executable software code for the execution of the recording of data to, or the reproduction of data from, a memory device, said code comprising:

A1 concl.

code for enciphering an enabling key block distribution authenticating key by an enabling key block comprising enciphering data for enciphering renewal keys on paths of a hierarchical key tree structure comprising a variety of keys disposed in correspondence with roots, nodes, and leaves of the key tree structure on paths ranging from roots to leaves of the key tree structure, and wherein a device is associated with one of the leaf keys, and wherein said enciphering data further comprises upper-rank keys to be enciphered by lower-rank keys; and

code for storing, in the memory device, a key distribution approval data file comprising header data, which comprises a link count key for designating a number of contents data that should be enciphered by the enciphering data acquirable from the enabling key block distribution authenticating key.